UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF 66 BRAGDON HILL ROAD POLAND, MAINE	Case No. 2:24-mj-144-KFW Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jason Leadbetter, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises for 66 Bragdon Hill Road, Poland, Maine hereinafter referred to as "PREMISES" further described in Attachment A, for the things described in Attachment A, for the things described in Attachment B.

2. As described in further detail below and in Attachment A, the government is seeking evidence inside and outside of the PREMISES known to be occupied by Target Subjects DEREK YOUNG and MARIA LAVASSEUR. The items to be seized by the government are described in further detail below and in Attachment B.

3. I have been assigned as a Task Force Officer with the Federal Bureau of Investigation ("FBI"), since January 2024, and am a sworn Portland Maine Police Detective. I have been employed to as a police officer with the Portland Police Department since August of 2010. Over the course of my law enforcement career, I have participated in numerous drug trafficking investigations, pursuant to which I have utilized various investigative tools and techniques, including search warrants.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other members of law enforcement and witnesses. This affidavit is intended to provide the facts necessary for a determination of probable cause for the requested search warrant.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that Target Subjects DEREK YOUNG, MARIA LEVASSEUR, and others unknown, are committing violations of Title 21, United States Code, Sections 841, 846, and 853 (drug trafficking, conspiracy to commit drug trafficking, and maintaining a drug-involved premises) and Title 18, United States Code Section 924(c) (possession of a firearm in furtherance of a drug trafficking crime), and that evidence of the these crimes will be found at the PREMISES. Accordingly, there is probable cause to search the PREMISES, more particularly described in Attachment A, for evidence of these crimes as further described in Attachment B.

PROBABLE CAUSE

6. The FBI and its law enforcement partners are conducting an ongoing covert criminal investigation into drug activity in and around the PREMISES perpetrated by YOUNG, LEVASSEUR, and their associates. In late February 2024, an FBI Confidential Source ("CS-1")[1] informed law enforcement that YOUNG was trafficking methamphetamine and fentanyl from the PREMISES.

---

[1] CS-1 is a paid informant who is cooperating with law enforcement for financial gain. CS-1 was previously convicted of cocaine trafficking in 2007. CS-1's information has been corroborated by, among other things, physical and electronic surveillance, and has been deemed reliable.

7. I know from my involvement in the investigation that on about February 29, 2024, law enforcement directed CS-1 to communicate with YOUNG to arrange a controlled purchase of fentanyl and cocaine base. Prior to the controlled buy, law enforcement met with CS-1, and equipped CS-1 with electronic monitoring and recording equipment. While under the direction and supervision of FBI, CS-1 called 207-346-7519 (which I know to be the call number associated with YOUNG's cellular phone, based upon information provided by CS-1) (hereinafter, the "YOUNG Phone")[2] and spoke to a male and arraigned the purchasing a "stick of down" and a "ball of up" for $500. Based on my training and experience, and based on information provided by CS-1, I know that "a stick of down" meant that the CS-1 wished to purchase 10 grams of fentanyl, and that a "ball of up" referred to 3.5 grams of cocaine or methamphetamine.

8. Once CS-1 had arranged the buy, law enforcement established surveillance at the PREMISES. Later that day, officers observed CS-1 arriving at the PREMISES, while monitoring the live audio feed transmitted from CS-1 equipment. CS-1 was heard on the monitoring equipment exiting the vehicle and entering the PREMISES. After a short interaction with a male inside the PREMISES, officers observed CS-1 driving away from the PREMISES.

9. Officers followed CS-1 to a pre-arraigned meeting location where they took possession of the illicit drugs from CS-1. CS-1 informed officers that inside the residence CS-1 observed a young Hispanic male, as well as YOUNG and LEVASSEUR. CS-1 stated

---

[2] It should be noted that, per information provided by the company Square, the call number associated with the YOUNG Phone is also associated with a Cash App account opened in YOUNG's name.

that YOUNG had served CS-1 the requested fentanyl and cocaine, which CS-1 had just turned over to FBI. I later field tested and weighed the illicit drugs which tested presumptively positive for fentanyl weighing 11.9ggw and cocaine base weighing 3.65ggw.

10. On about March 5, 2024, at the direction of FBI, CS-1 made a recorded phone call to the YOUNG Phone and spoke to a male. CS-1 again placed the same order, for a "stick" and a "ball." CS-1 was again equipped with electronic recording and transmitting devices, and law enforcement again set physical surveillance of the PREMISES. While monitoring CS-1's transmitting equipment, officers overhead CS-1 exit the vehicle and approach the PREMISES. A short time later CS-1 was surviellled leaving the location. Law enforcement followed CS-1 back to a pre-determined location where CS-1 turned over the illicit drugs CS-1 had just purchased. CS-1 reported that YOUNG again served CS-1 the fentanyl and crack. During the transaction, CS-1 observed that YOUNG was cooking powdered cocaine into crack cocaine. CS-1 also stated that he observed a handgun, which YOUNG told CS-1 was a Hi-Point 9mm. Officers later field tested and weighed the narcotics purchased by CS-1; they tested presumptively positive for fentanyl weighing 10.25ggw and cocaine base weighing 4.6ggw.

11. On about March 21, 2024, at the direction of law enforcement, CS-1 called YOUNG on the YOUNG Phone and arranged to the purchase a gram of fentanyl, methamphetamine and handgun from YOUNG. Law enforcement equipped CS-1 with electronic recording and transmitting devices and then set physical surveillance at the PREMISES. Law enforcement observed CS-1 arrive at the PREMISES, and then minutes later, depart the PREMISES. Officers followed CS-1 to a pre-determined location, at which time, they met with CS-1. CS-1 reported that LEVASSEUR served the drugs to CS-1 on this occasion, and that afterwards, CS-1 observed LEVASSEUR go into a room

where C-1 overheard a number of individuals CS-1 believed to be Dominican. YOUNG was present in that room cooking powdered cocaine into crack cocaine. CS-1 observed two .45 pistols, a 9mm rifle, and two .357 revolvers. YOUNG told CS-1 that the .45s were $1,000 each and .357s were $275 each. CS-1 elected to purchase the .357 revolver. After providing this information, CS-1 provided law enforcement with suspected fentanyl, methamphetamine and a Mag Pug .357 revolver manufactured by Charter Arms that CS-1 had purchased at the PREMISES. Officers subsequently field tested and weighed the illicit drugs, which tested presumptively positive for fentanyl and weighed 2.7ggw and methamphetamine which weighed 29.35ggw. Agents of the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") have conducted a trace report on the firearm, from which I have learned that it was purchased by a third party in 2016. I know from reviewing open-source information that all Charter Arms firearms are manufactured in Connecticut.

12. On about April 17, 2024, at the direction of FBI, CS-1 again called YOUNG on the YOUNG Phone and arranged to buy two ounces of methamphetamine and a handgun. CS-1 was then equipped with electronic monitoring and recording devices, and officers set physical surveillance of the PREMISES. CS-1 was surveilled arriving at the PREMISES, entering the PREMISES, and staying for several minutes before exiting the PREMISES. Law enforcement then followed CS-1 to a pre-determined location. CS-1 informed officers that YOUNG, LEVASSEUR , and Target Subject CHELSEA DUGUAY were present at the PREMISES. YOUNG told CS-1 that he had already sold the semiautomatic pistol that CS-1 had wanted to purchase. CS-1 expressed disappointment, and then asked YOUNG for a couple ounces of methamphetamine, which he provided to CS-1 for $700. After providing this information, CS-1 turned over the suspected

methamphetamine to law enforcement. Officers subsequently field tested and weighted the illicit drug, which tested presumptively positive for methamphetamine weighing 58.85ggw.

13. On about April 24, 2024, at the direction of law enforcement, CS-1 again called YOUNG at the call number associated with the YOUNG Phone. YOUNG informed CS-1 that he had a "hammer" for CS-1 and that it was a 9. I know from my training and experience, and from conversations with CS-1, that when YOUNG stated that he had a "hammer," he meant that he had a firearm for CS-1; "9" referred to the fact that the firearm was a 9 mm pistol. CS-1 was then equipped with electronic monitoring and transmitting devices, and agents again established surveillance of the PREMISES. CS-1 was surveilled arriving at the PREMISES, staying for several minutes, and then exiting the PREMISES, at which point law enforcement followed CS-1 to a pre-determined location. CS-1 reported that YOUNG and LEVASSEUR were present within the PREMISES. CS-1 further reported that CS-1 handed YOUNG $500 in prerecorded buy money, and that in exchange, YOUNG handed CS-1 a plastic handgun box. CS-1 observed cocaine powder and crack cocaine on the living room table and a long gun and handgun were present in the room. After the debrief, CS-1 handed me the plastic handgun box, which contained a 9mm SCCY CPX-2 handgun with eight 9mm rounds in the loaded magazine. ATF agents conducted a trace analysis of the firearm, showing that it was purchased in Maine by a third party in 2021. I know from reviewing open-source information that all SCCY firearms are manufactured in Florida.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

14. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are

found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

15. *Probable cause*. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations,

artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

16. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

17. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically

also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

18. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or

months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

19. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

20. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

Jason Leadbetter
Task Force Office
Federal Bureau of Investigation

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedures

Date: May 03 2024

City and state: Portland, Maine

Judge's signature

Karen Frink Wolf, U.S. Magistrate Judge
Printed name and title